Seeing beyond

ZEISS Cybersecurity and Data Privacy Governance Program

ZEISS Imaging and Diagnostic Systems

ZEISS Humphrey Field Analyzer

ZEISS CIRRUS OCT

ZEISS CLARUS Fundus Camera

As the digitalization of healthcare evolves, the landscape of cybersecurity threats is also evolving. Securely protecting products and data across the connected care environment is critical. Through our ZEISS Cybersecurity and Data Privacy Governance Program, we manage security risks across the product lifecycle and monitor the digital landscape to protect the security of our products from emerging threats and vulnerabilities.

SIMPLE STEPS

Keeping your ZEISS imaging and diagnostic systems secure

- **Software updates:** Ensure your ZEISS device software and operating system are regularly updated to patch known vulnerabilities.
- **User authentication and role-based access control:** ZEISS devices employ username and password-based authentication for both Windows OS and the device application. They support multiple user roles with varying levels of access, including administrator, service, and general user accounts, ensuring that only authorized personnel can access sensitive data and system configurations.
- **Enhanced security settings:** ZEISS devices come with enhanced security settings enabled by default, which include firewall rules, screen saver/lock screen configurations, Windows Defender, and password policies. These settings help minimize the attack surface and protect the device from unauthorized access.
- **Audit and logging:** ZEISS device software logs important user activities, errors, and network requests, creating an audit trail that can be used for security monitoring and forensic analysis. This includes logging of logon/logoff events, data modifications, and remote service activities.
- **Data protection:** Patient data stored on ZEISS devices is secured with a secret password, and the device is compatible with BitLocker for drive encryption. Additionally, communication between your ZEISS device and DICOM solutions can be encrypted using DICOM TLS, ensuring secure data transmission.

For access to all approved patches* and updates visit:
www.zeiss.com/cybersecurity

*Access to available patches for ZEISS imaging and diagnostic systems is restricted to MyZEISS registered users. To register, visit: **www.zeiss.com/meditec/us/myzeiss.html**